1. OBJETO:

Describir el proceso para la identificación, recolección y adquisición de evidencia digital que asegure su integridad y autenticidad, mitigando el riesgo de alteración para su posterior investigación y análisis forense para respuesta a incidentes de ciberseguridad.

2. ALCANCE:

El protocolo aplica para todos los funcionarios y contratistas involucrados en la recolección y adquisición de evidencias digitales en incidentes cibernéticos.

Este protocolo se aplica a los siguientes tipos de evidencia digital y dispositivos propiedad de la UAESP:

- Discos duros
- Memorias USB
- Memoria RAM
- Tarjetas SD
- Computadores de escritorio
- Laptops
- Servidores On-premise (Físicos o Virtuales)

3. DEFINICIONES:

Adquisición de evidencia digital: Consiste en generar una réplica exacta de datos dentro de un entorno previamente determinado.

Cadena de Custodia: El proceso de documentación que asegura el control, transferencia, análisis y disposición de la evidencia desde el momento de su recolección hasta su presentación en un proceso legal.

Copia Bit a Bit: Proceso de creación de una réplica exacta y completa de un dispositivo de almacenamiento, en el cual se copian todos los bits de datos, tanto asignados como no asignados. La copia bit a bit también se denomina copia física.

DEFR (Digital Evidence First Responder): Individuo que puede desempeñar las funciones de un DEFR y cuenta con conocimientos especializados, habilidades y capacidades para abordar una variedad de problemas técnicos.

DES (Digital Evidence Specialist): Individuo que puede desempeñar las funciones de un DEFR y cuenta con conocimientos especializados, habilidades y capacidades para abordar una variedad de problemas técnicos.

Embalado: Disponer en balas o colocar convenientemente dentro de cubiertas la evidencia digital que han de transportarse o almacenarse.

Evidencia Digital: Información o datos, guardados o transmitidos en formato binario, que pueden considerarse confiables como prueba.

Recolección: recolección de objetos físicos que contienen evidencia digital potencial.

Rotulado: Etiquetar cada dispositivo de manera clara, por medio del formato dispuesto, en el cual se incluye un identificador único que se refleje en la documentación de la cadena de custodia, fecha, hora, nombre del investigador, descripción de la evidencia.

Snapshot: Copia completa de solo lectura de un disco duro virtual (VHD).

Suma de Verificación (Valor Hash): Cadena única generada a partir de datos mediante una función hash criptográfica. Se utiliza para verificar la integridad de los datos.

Verificación de la Imagen: Verificar que la imagen adquirida sea una réplica exacta del dispositivo original comparando los valores hash.

Volatilidad de los Datos: La susceptibilidad de los datos a ser alterados, perdidos o destruidos debido a factores como el tiempo, la temperatura o la manipulación inadecuada.

4. PRINCIPIOS FUNDAMENTALES

4.1. Minimización del Manejo

La manipulación directa de dispositivos digitales originales debe ser mínima para prevenir alteraciones o daños a la evidencia. Siempre que sea posible, se deben utilizar copias forenses o bit a bit en lugar de los dispositivos originales.

4.2. Documentación Detallada

Todas las acciones, decisiones y observaciones realizadas durante el manejo de evidencia digital deben ser documentadas de manera exhaustiva y precisa. Esta documentación es crucial para garantizar la trazabilidad y la efectividad del análisis durante la respuesta a incidentes.

4.3. Consideraciones sobre la privacidad

No realice ningún procedimiento sobre equipos personales de funcionarios o contratistas, podría estar violando la privacidad de las personas aún con consentimiento oral o escrito.

Si existe indicios de posible evidencia digital decisiva en dispositivos móviles personales y es un incidente grave o muy grave, considere una denuncia ante las autoridades competentes y entregue las demás evidencias como prueba.

4.4. Transparencia

Todas las técnicas y procedimientos empleados en la recolección y adquisición de evidencia digital deben estar claramente documentados y ser accesibles, de manera que otros expertos puedan replicar el proceso y obtener los mismos resultados. Esto es especialmente crucial en situaciones donde una respuesta a incidentes derive en una

investigación judicial, asegurando así la integridad y validez de las pruebas presentadas.

5. ROLES Y RESPONSABILIDADES

En el marco de investigación de incidentes de ciberseguridad es importante definir los roles mínimos necesarios para realizar las etapas de investigación forense, estos roles dependerán del conocimiento y capacidades.

TABLA 1 ROLES Y RESPONSABILIDADES

ETAPA	ROL	RESPONSABILIDADES
Notificación y Evaluación inicial	- Oficial de Seguridad de la Información. - Jefe Oficina TIC	Recibir la notificación del incidente y coordinar la evaluación inicial. Decidir si es necesario activar al DEFR y al DES.
Identificación	DEFR: Soporte técnico I y II	Realizar la identificación inicial de la evidencia digital, priorizando la recolección de datos volátiles. Documentar la escena y asegura la evidencia.
Recolección	DEFR: Soporte técnico I y II	Recolectar evidencia volátil utilizando herramientas apropiadas y la transfiere al DES para la adquisición.
Adquisición	DEFR / DES: Oficial de Seguridad o Soporte Técnico II	Realizar la adquisición de la evidencia digital no volátil utilizando herramientas forenses, asegurando la integridad de esta.

Fuente: Elaboración propia

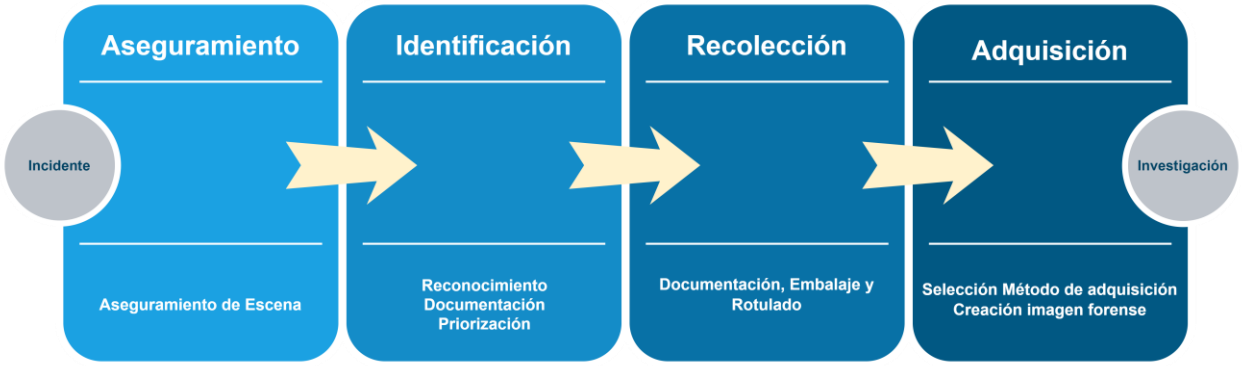
El personal con roles DES (Especialista en Evidencia Digital) podrá apoyar a los DEFR o primer respondiente en las tareas relacionadas con adquisición cuando así lo requieran por experticia en manejo de herramientas, volúmenes de elementos con evidencia digital potencial o procedimientos de informática forense.

6. PROTOCOLO DE ACTUACIÓN Y TAREAS

El protocolo para gestión de Evidencia Digital Forense se compone de cinco fases: Aseguramiento, Identificación, Recolección, Adquisición y Preservación.

Este protocolo describe las primeras 4 etapas de acuerdo con la siguiente ilustración:

Ilustración 1 Fases del Protocolo de gestión de la evidencia digital



Fuente: Elaboración propia

6.1. Fase: Asegurar la Escena

Antes de iniciar con la fase de identificación, es importante que el primer respondiente o DEFR asegure el área:

A. Acordónela o delimítela de forma que se puedan realizar las primeras fases evitando contaminación o posible alteración de la evidencia por parte de un tercero.

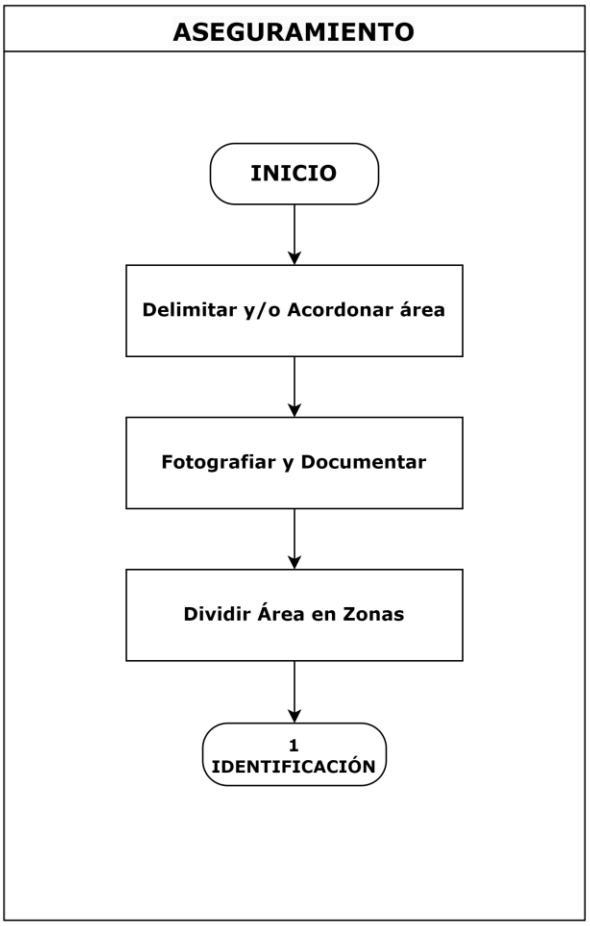
B. Tome fotografías del área y documente las decisiones tomadas durante todo el procedimiento.

Nota 1: Si considera necesario, solicite apoyo de personal de vigilancia para realizar las siguientes fases sin interrupción de un tercero no autorizado.

Nota 2: Si el área es muy grande, divida el área en zonas más pequeñas ayudándose de una línea imaginaria o trazando con un lazo o soga.

6.1.1. Diagrama

Ilustración 2 Diagrama de flujo fase de aseguramiento



Fuente: Elaboración propia

6.2. Fase: Identificación de la Evidencia

El primer paso en la fase de gestión de evidencia digital forense es la identificación, esto implica buscar todas las posibles fuentes donde reposen o exista posible evidencia digital en relación con el incidente de ciberseguridad.

Para lo anterior realice:

A. Una inspección visual del lugar para identificar todos los dispositivos digitales presentes como:

• Dispositivos de almacenamiento: Discos duros, CD's, unidades flash, tarjetas de memoria, unidades externas, redes de almacenamiento, dispositivos de almacenamiento físicos o virtualizados, entre otros.

• Dispositivos móviles: Computadoras, teléfonos móviles, tabletas, entre otros.

• Dispositivos IoT: Cámaras de seguridad, asistentes virtuales, control de acceso, entre otros.

• Servidores (Físicos o virtuales).

• Cualquier otro elemento relacionado con el incidente de ciberseguridad.

B. Registre la ubicación, estado (encendido/apagado), formato y hora del sistema y características de cada dispositivo identificado.

C. Utilice formularios estandarizados para la documentación, incluyendo fotos y descripciones detalladas.

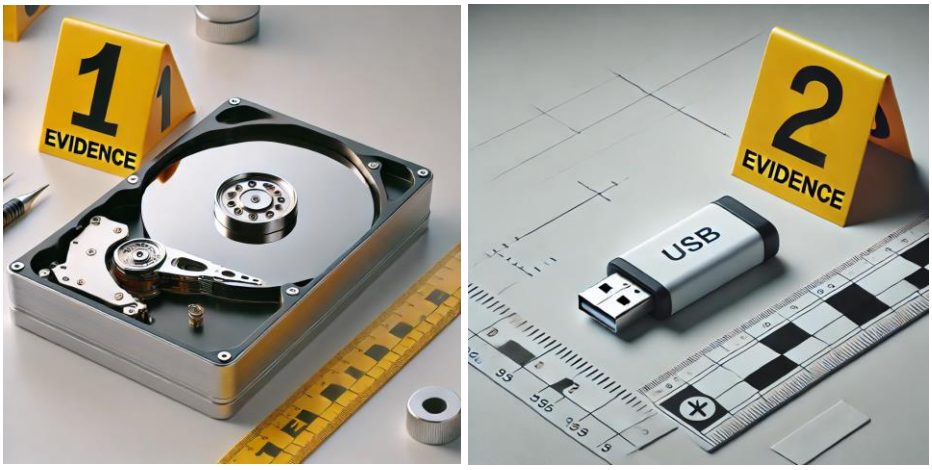
D. Busque dispositivos ocultos o disimulados entre otros objetos.

E. Evalúe la volatilidad de los datos para determinar el orden de recolección. Los datos más volátiles deben ser recolectados primero para evitar su pérdida.

Una vez identificada las fuentes con posibles evidencias digitales se debe definir si se recolectan o adquieren de acuerdo con la volatilidad o relevancia de los datos que aseguren maximizar la cantidad de evidencia digital potencial.

Así mismo, enumere las evidencias encontradas y priorizadas con ayuda de numeradores y testigos métricos como se ilustra a continuación.

Ilustración 3 Numeración de evidencias



Fuente: Generada con OpenAI (2024)

6.2.1. Criterios de volatilidad.

Debido a la naturaleza efímera de los datos volátiles, es fundamental adquirirlos de manera inmediata y prioritaria según su nivel de volatilidad. El siguiente esquema en forma de pirámide muestra cómo los diferentes tipos de evidencia digital deben ser manejados en función de su volatilidad, desde los más volátiles en la cúspide hasta los menos volátiles en la base:

Ilustración 4 Orden de Volatilidad de la evidencia

Fuente: Elaboración propia

Use la siguiente tabla como ayuda para decidir entre la recolección y adquisición de evidencia digital.

TABLA 2 ACCIONES PARA LA GESTIÓN DE EVIDENCIA DIGITAL

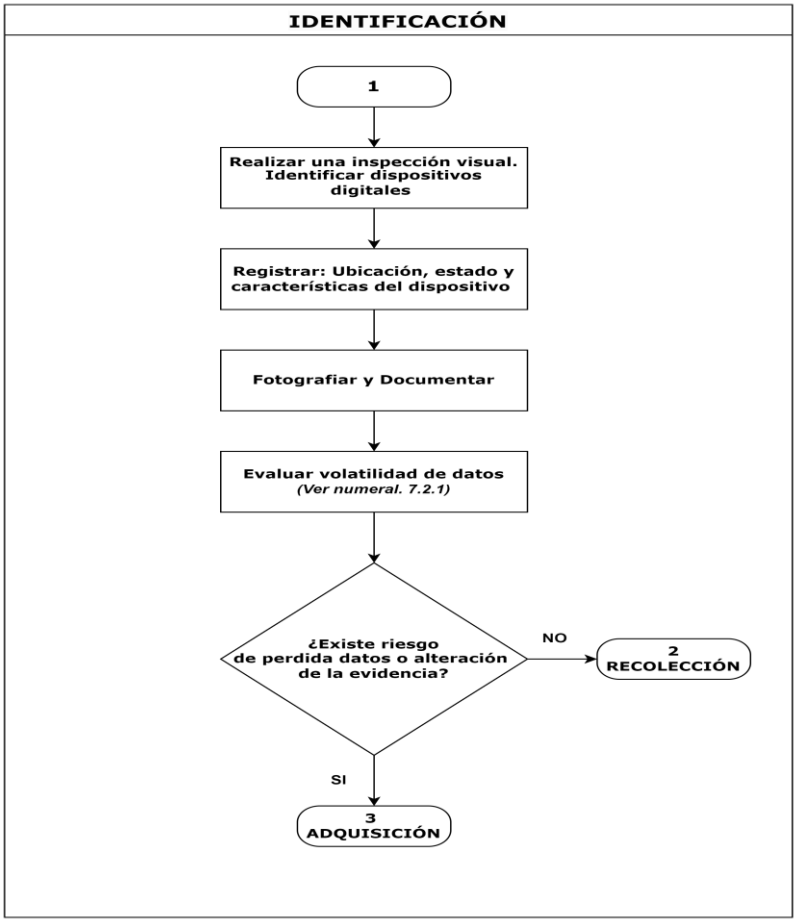
Elemento	Estado	Acción	Volatilidad	Herramientas
Memoria RAM	Equipos Encendidos (Computadoras	Adquisición	Volátil	- FTK Imager - Volatility - LiME

Elemento	Estado	Acción	Volatilidad	Herramientas
	– Servidores)			-dd
Procesos en ejecución	Equipos Encendidos (Computadoras – Servidores)	Adquisición	Volátil	- Volatility - LiME -dd
Conexiones de Red Activas	Equipos Encendidos (Computadoras – Servidores)	Adquisición	Volátil	- Wireshark - netstat
Sistemas de Archivos y directorios	Equipos encendidos/apagados, discos duros.	Recolección.	No volátil	- Autopsy - The Sleuth Kit
Dispositivos USB – Discos duros	Conectados	Adquisición	No volátil	- Guymager
Dispositivos USB – Discos duros	Desconectados	Recolección	No volátil	- Guymager
Cámaras IP y CCTV	Encendidos	Adquisición	No Volátil	- Appliance de dispositivos. - Wireshark.
Dispositivos IOT	Encendidos	Adquisición	Volátil	- Wireshark - tcpdump
Teléfonos Móviles Tabletas	Encendidos	Adquisición	Volátil	- AFLogical OSE - Magnet ACQUIRE Community Edition - Autopsy
	Apagado	Recolección	No volátil	

Fuente: Elaboración propia.

6.2.2. Diagrama

Ilustración 5 Diagrama de flujo etapa fase de identificación



Fuente: Elaboración propia

6.3. Fase: Recolección

La recolección es el proceso donde los elementos que pueden tener evidencia digital potencial son removidos de su ubicación original y son trasladados al DataCenter o donde se ubique un posible laboratorio forense para posterior análisis dentro de la respuesta a incidentes.

Para lo anterior, realice:

A. Documente el estado del dispositivo antes de la recolección. Esto implica tomar fotografías y anotar detalles relevantes como la ubicación, el número de serie, marca, modelo y cualquier otra característica relevante.

B. Use accesorios antiestáticos durante la manipulación de la evidencia digital.

- Guantes de látex.

- Manilla antiestática.

C. No apague equipos si están encendidos o viceversa, considere primero el riesgo de perder información por la volatilidad de los datos del numeral 6.2.1 y de ser necesario realice la adquisición primero, numeral 6.4.

D. Embale cada dispositivo físico en contenedores a prueba de golpes de ser posible o use envoltorios como plástico burbuja.

E. Rotule cada evidencia de manera clara, incluyendo un identificador único que se refleje en la documentación de la cadena de custodia.

   Para el identificador use el mismo número del ticket de mesa de servicio seguido de un guion y el numero de la evidencia.

   Ejemplo: 0001234-001

   0001234: Numero de ticket.

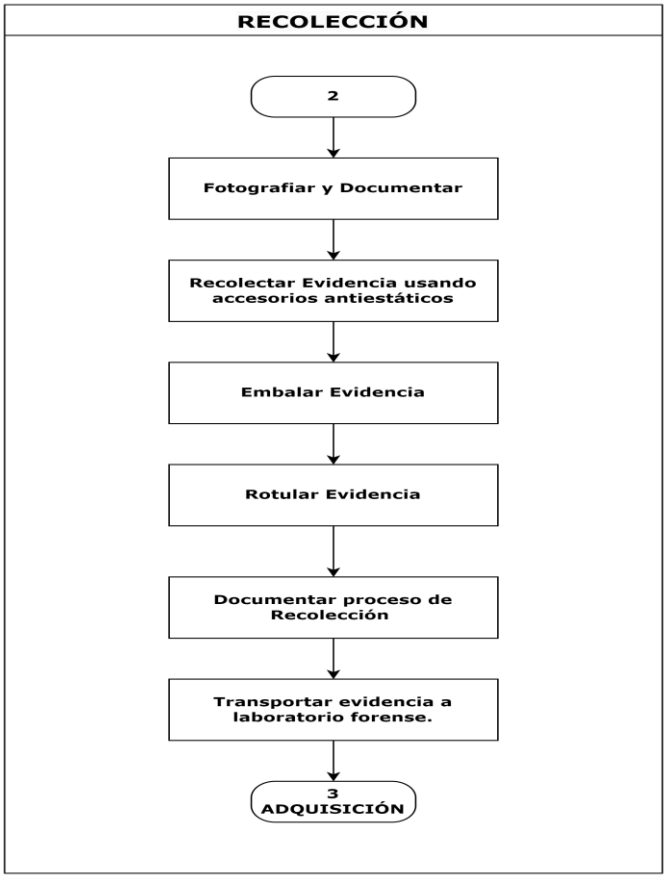
   001: Numero o Identificación de la evidencia.

   Pegue el rotulo al embalaje de la evidencia.

F. Transporte la evidencia al DataCenter o donde se realice el análisis forense, asegurando que el traslado se haga de manera que minimice el riesgo de daños o alteraciones.

6.3.1. Diagrama

Ilustración 6 Diagrama de flujo fase de recolección



Fuente: Elaboración propia

6.4. Fase: Adquisición

El proceso de adquisición involucra la copia de la evidencia digital y la documentación de los métodos o procedimientos usados y realizados.

Para lo anterior, realice:

A. Proceda desde el elemento más volátil al menos volátil de acuerdo con el numeral 6.2.1.

B. Evalúe si la adquisición debe ser física (copia bit a bit o copia completa del disco) o una adquisición lógica (copia de archivos o particiones específicas).

C. Utilice herramientas de adquisición para crear la imagen forense del dispositivo.

   Apóyese en la tabla 3 para la selección de la mejora herramienta de acuerdo con la experiencia o conocimiento del DES.

D. Genere y documentar el hash de la imagen adquirida.

E. Realice Verificación de la imagen adquirida para comprobar la integridad de esta.

   Windows:

   - Instrucción en powershell: Get-FileHash -Algorithm SHA256 "ruta\del\archivo"
   - Use herramientas como “hash tool” de Microsoft Store.

   Linux:

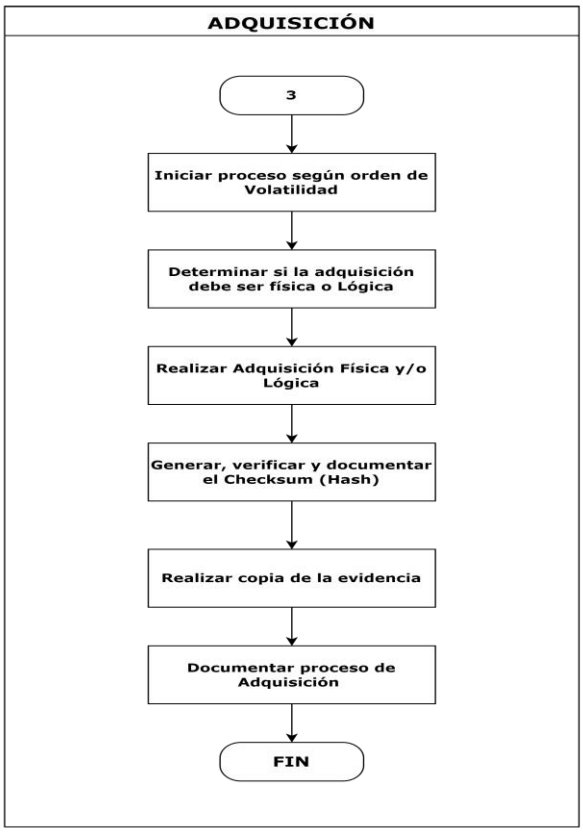
   - Línea de comandos: shasum -a 256 “nombre_del_archivo”

F. Siempre que sea posible, tome una segunda copia sobre la primera y compruebe el hash. Esto permitirá trabajar con una copia sin comprometer el original y asegurar la validez en un posible proceso legal.

   Registre el proceso de adquisición, incluyendo la fecha, hora, herramientas utilizadas, y cualquier incidencia durante el proceso.

6.4.1. Diagrama

Ilustración 7 Diagrama de lujo fase adquisición



Fuente: Elaboración propia

7. HERRAMIENTAS.

A continuación, se listan las herramientas *Open Source* que pueden usarse para la adquisición y posterior análisis de evidencia digital de acuerdo con el dispositivo, plataforma y propósito de estas.

TABLA 3 HERRAMIENTAS PARA ADQUISICIÓN

Herramienta	Sitio Oficial	Sistema Operativo	Propósito Principal	Dispositivos
FTK Imager	https://www.exterro.com/digital-forensics-software/ftk-imager	Windows	Creación de imágenes forenses de discos y adquisición de memoria RAM	Discos duros, particiones Memoria RAM Archivo de Paginación
dd	Preinstalada	Linux / Unix, macOS	Copiar datos a bajo nivel en	Memoria RAM Discos Duros

Herramienta	Sitio Oficial	Sistema Operativo	Propósito Principal	Dispositivos
			sistemas Linux/Unix.	Particiones
Guymager	https://guymager.sourceforge.io/	Linux	Adquisición de imágenes forenses de discos	Discos Duros
Wireshark	https://www.wireshark.org/	Linux, macOS, Windows	Captura y análisis de tráfico de red	Dispositivos de red
tcpdump	https://www.tcpdump.org/	Linux, macOS, Unix	Captura de tráfico de red en tiempo real	Dispositivos de red
Volatility	https://volatilityfoundation.org/	Multiplataforma (Linux, Windows, macOS)	Análisis y adquisición de memoria RAM	Memoria RAM

Fuente: Elaboración propia.

8. CONTROL DE CAMBIOS

TABLA 4 CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
01	18/10/2024	Creación del documento

Fuente: UAESP

9. AUTORIZACIONES

TABLA 5 AUTORIZACIONES

	NOMBRE	CARGO	FIRMA
Elaboró	Juan Sebastián Perdomo Méndez	Profesional Universitario Oficina TIC	
Revisó	Jorge Alexis Rodriguez Meza	Jefe Oficina TIC	
Aprobó	Luz Mary Palacios Castillo	Jefe Oficina Asesora de Planeación (E)